Formal Development and Verification of Safe Railway Control Systems

Haxthausen, Anne Elisabeth; Vu Hong, Linh

Publication date:
2013

Document Version
Publisher's PDF, also known as Version of record

DTU Compute
Department of Applied Mathematics and Computer Science

Formal Development and Verification of Safe Railway Control Systems

Challenges

Before 2021 all Danish signalling systems are going to be replaced with modern computer based systems. Central parts of these systems consist of *safety-critical software*.

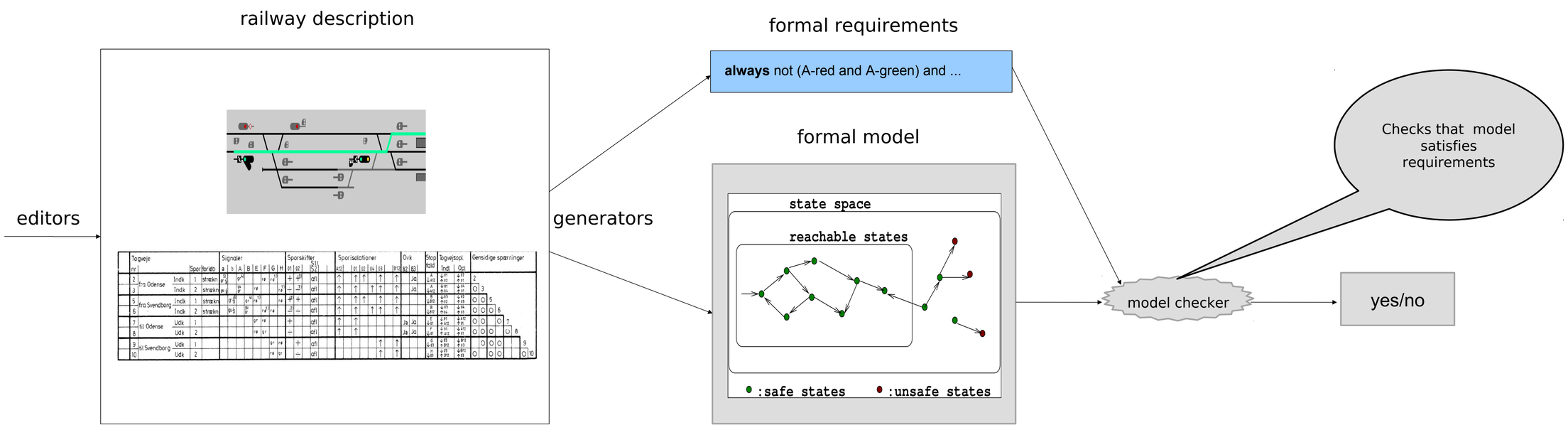
Challenges: How to develop such new systems *efficiently* (i.e. cheap and fast) and at the same time ensure that they are *safe*?

Research Goals of a Forthcoming PhD project

Research how to provide efficient methods and tools for development of safe railway control software.

The main approach to achieve this is to use of *automation* and *formal methods.*

Solution Ideas



Key idea is to provide:

- railway domain-specific language
- re-usable formal requirements and models
- tools for automated generation of concrete, formal requirements and models from domain-specific descriptions
- techniques and tools for formal, automated verification

RobustRailS

Anne Haxthausen, DTU Compute, aeha@dtu.dk
Linh Vu Hong, DTU Compute, lvho@dtu.dk

DET STRATEGISKE FORSKNINGSRÅD
Danish Agency for Science Technology and Innovation
Ministry of Science, Innovation and Higher Education